SECURITY AND PRIVACY WHITE PAPER

Poly Lens cloud service, Lens Desktop app, and Lens Mobile app

Part 3725-86286-001

Version 10

March 2024

Introduction

This white paper addresses security and privacy related information for the Poly Lens cloud service as well as Lens Desktop app and Lens Mobile app.

This paper also describes the security features and access controls in HP | Poly's processing of personally identifiable information or personal data ("personal data") and customer data in connection with the provisioning and delivery of the Poly Lens service and related apps, and the location and transfers of personal and other customer data. HP | Poly will use such data in a manner consistent with the HP Privacy Statement, and this white paper which may be updated from time to time. This white paper is supplemental to the HP Privacy Statement. The most current version of this white paper will be available on HP | Poly's website. You may also subscribe to receive notifications when this paper is updated from the website.

Poly Lens provides an enrolled customer with access to a dedicated web portal which includes device management of Poly conferencing endpoints and basic reporting capabilities. Reports are based on data (including certain personal data of a customer as described below) collected from a customer's Poly endpoints that are configured to send data to HP | Poly. Customer data is automatically uploaded to Poly Lens and accessed via the Poly Lens web portal application using an encrypted tunnel and software module embedded in the endpoints.

Poly Lens Desktop app is a powerful app for customizing your personal devices, staying up to date with the latest software, and accessing helpful tips and support with a touch. The Poly Lens Mobile app allows you to manage Poly Bluetooth headsets and personal speakerphones to help you get the most out of your Poly devices.

Security at HP | Poly

Security is always a critical consideration for a cloud-based service such as Poly Lens and its related apps. HP | Poly's Information Security Management System (ISMS) has achieved ISO 27001:2013 certification. ISO/IEC 27001 is the most widely accepted international standard for information security best practices and you can be reassured that HP | Poly has established and implemented best-practice information security processes.

Product security at HP | Poly is managed through the HP Cybersecurity team, which oversees secure software development standards and guidelines. The HP | Poly Product Security Standards align with NIST Special Publication 800-53, ISO/IEC 27001:2013, and OWASP for application security. Guidelines, standards, and policies are implemented to provide our developers with industry approved methods for adhering to the HP | Poly Product Security Standards.

Secure Software Development Life Cycle

HP | Poly follows a secure software development life cycle (S-SDLC) with an emphasis on security throughout the product development processes. Every phase of development process ensures security by establishing security requirements alongside functional requirements as part of initial design. Architecture reviews, code reviews, internal penetration testing and attack surface analysis are performed to verify the implementation.

The S-SDLC implemented by HP | Poly also includes a significant emphasis on risk analysis and vulnerability management. To increase the security posture of Poly products, a defense-in-depth model is systematically incorporated through layered defenses. The principle of least privilege is always followed. Access is disabled or restricted to system services nonessential to standard operation.

Standards-based Static Application Security Testing (SAST) and patch management are cornerstones of our S-SDLC.

Privacy by Design

HP | Poly implements internal policies and measures based on perceived risks which meet the principles of data protection by design and data protection by

default. Such measures consist of minimizing the processing of personal data, anonymizing personal data as soon as possible, transparently documenting the functions, and processing of personal data and providing features which enable the data subject to exercise any rights they may have.

When developing, designing, selecting, and using applications, services and products that are based on the processing of personal data or process personal data to fulfill their task, HP | Poly considers the right to data protection with due regard.

Security by Design

HP | Poly follows Security by Design principles throughout our product creation and delivery lifecycle which includes considerations for confidentiality, integrity (data and systems) and availability. These extend to all systems that HP | Poly uses – both on-premises and in the cloud as well as to the development, delivery and support of Poly products, cloud services and managed services.

The foundational principles which serve as the basis of HP | Poly's security practices include:

1. Security is required, not optional
2. Secure by default, Secure by design
3. Defense-in-depth
4. Understand and assess vulnerabilities and threats
5. Security testing and validation
6. Manage, monitor, and maintain security posture
7. End-to-end security: full lifecycle protection

Security Testing

Both static and dynamic vulnerability scanning as well as penetration testing are regularly performed for production releases and against our internal corporate network by both internal and external test teams.

Cloud systems are managed by HP | Poly and are updated as needed. Patches are evaluated and applied in a timely fashion based on perceived risk as indicated by CVSSv3 scores.

Change Management

A formal change management process is followed by all teams at HP | Poly to minimize any impact on the services provided to the customers. All changes implemented for the Poly Lens service and related apps go through vigorous quality assurance testing where all functional and security requirements are verified. Once Quality Assurance approves the changes, the changes are pushed to a staging environment for UAT (User Acceptance Testing). Only after final approval from stakeholders, changes are implemented in production. While emergency changes are processed on a much faster timeline, risk is evaluated, and approvals are obtained from stakeholders prior to applying any changes in production.

Data Processing

HP | Poly is the processor of customer data while the customer is the data controller.

Poly group or room conferencing devices automatically send product usage data, device data, call detail records (CDRs), and quality of service data to Poly Lens. To turn OFF data collection, please see the Privacy Guide and Administrator's Guide for your device.

Poly personal or desktop devices do not send data by default and must be configured by the device administrator to do so.

Similarly, Lens Desktop and Lens Mobile apps do not send data by default and also must be configured by the admin or user to do so. Please see the applicable Administrator's Guide for each app.

HP | Poly has access to customer personal data that is sent to Poly Lens when Poly devices and/or apps are configured to do so. Customer personal data may also be reported to an internal analytics service used for product improvement purposes.

	Source from Where PI Collected	Categories of PI Collected	Business Purpose for Collection	Disclosed to the following Service Providers
Lens cloud service	• Device Administrator and user information	• First/Last Name • User ID • SIP username • SIP alias name • Email address • Password (hashed) • Organization name • Tenant ID	• Authenticate and authorize administrative access to the service • Deliver the service • Reporting • Usage/activity	Auth0, Azure, AWS
	• Device Identifier and Network data	• Device ID • Device name • MAC address (for both primary device and paired/ unpaired IP peripherals) • Serial number • Software version • IPv4/v6 address • SIP address • MAC address • Display name • System name • System owner • Domain name • Log files • Device geolocation data including time zone • Network identifiers • Network type • Bluetooth addresses • Device status • Device configuration records	• Understand how devices are being used in a customer environment • Help customer diagnose technical issues • Collect analytics to improve the technical performance of the customer's UC service • Provide details in support of room or devices issues that require support • Serial number for entitlement	Azure, AWS
	• Local and Remote Call Participant Information	• Full Call detail record (CDR) • Dial string number • Call ID • Participant names (local and remote) • Participant IP addresses (local and remote)	• Customer identification of specific troubled calls • Short-term, transient use (login)	Azure, AWS

	Source from Where PI Collected	Categories of PI Collected	Business Purpose for Collection	Disclosed to the following Service Providers
Lens Desktop App	User information	• User ID • User email address • Username • IP address of user desktop computer	• Authentication to Lens Cloud account • General settings display	Auth0, Azure, AWS
	Device management and IoT information	Device ID of each attached USB peripheral device	Device management	Azure, AWS
	Call information	• Call information (duration and provider network) • Desktop environment settings	• Troubleshooting • Product improvement	Azure, AWS

	Source from Where PI Collected	Categories of PI Collected	Business Purpose for Collection	Disclosed to the following Service Providers
Lens Mobile App	Location information	Specific location of mobile device (not headset)	• Find My Device feature (if enabled by user)	None (local only)
	Analytics	• Crash dump • Log files	• Troubleshooting • Crash analytics	Google (Firebase)
	User information	• User ID • User email address • Username • Authentication token (stored in protected • keychain)	• Authentication to Lens Cloud account • General settings display	Auth0, Azure, AWS
	Device management and IoT information	• Device ID • Tenant ID	• Device management	Azure, AWS

Poly Lens cloud service also collects and processes logs containing:

- Device data (includes details such as type of device, device name, installed software version, etc.)
- CDR data (includes call connection information such as IP addresses, phone numbers, call ID, local and remote call participant names, etc.)

NOTE: When a Poly video device is in third party mode (Teams, Zoom, RingCentral, etc.). Poly Lens only receives call-start and call end information, which allows lens to say how long a device was in use and what provider was used. This is NOT the same CDR information as received when a Poly video device places a standards-based SIP or H.323 call.

If someone is an individual user, and the purchase of Poly Lens has been made by their employer as the customer, all the privacy information relating to personal data in this white paper is subject to their employer's privacy policies as controller of such personal data.

Purpose of Processing

The primary purpose of processing information with Poly Lens service is to:

- Enable inventory management—View your devices and manage important information like software versions and device data.
- Perform data analytics—Better understand utilization, performance, and call quality.

NOTE: Personal data is processed for display and reporting purposes only.

How Customer Data is Stored and Protected

Poly Lens cloud service stores customer data in Azure and AWS databases. Data is encrypted at rest using AES 256. Data resides in the United States. Data is sent via encrypted IoT messages to Azure's East US 2 datacenter in Boydton, Virginia. It is then cached in microservices that run in the AWS Oregon regional datacenter (near Umatilla). Persistent telemetry is stored in an Azure data lake in Azure West US 2 (Washington State).

The Poly Lens database servers are in SSAE 16 Type II certified data centers in the United States that run dedicated databases and application servers. When the Poly Lens database servers receive data from the customer, it is verified for integrity, processed, and saved in the databases.

HP | Poly may change the location of the Poly Lens database servers and details of any such change shall be set forth in the latest copy of this white paper available on HP | Poly's website. You may also subscribe to receive notifications when this paper is updated from the website.

For transferring personal data of EU customers to the US, HP | Poly uses an Intragroup Data Transfer Agreement incorporating the EU Standard Contractual Clauses as the transfer mechanism.

The Poly Lens databases and application servers reside in data centers behind a fully patched firewall that is also managed. Access for any services not required by Poly Lens is blocked.

Data Deletion and Retention

All information collected from the customer is stored in the database with the tenant information configured as the access control mechanism. Nothing is transmitted outside of the Poly Lens cloud service. All data is self-contained in the database in the data center.

HP | Poly may retain customer data for as long as needed to provide the customer with any Poly cloud services for which they have subscribed and for product improvement purposes. When a customer makes a request for deletion to HP's Chief Privacy and Data Protection Officer form, HP | Poly will delete the requested data within 30 days, unless the data is required to be retained to provide the service to customer. HP | Poly may "anonymize" personal data in lieu of deletion. In cases where anonymization occurs, the process is irreversible and includes but is not limited to searching and sanitizing all customer-specific data (e.g., name, site information, and IP address) with randomly generated alphanumeric characters.

Cryptographic Security

Data at rest for the Poly Lens cloud service is protected using standard AES-256 cipher suites as well as hash strengths including SHA-256, SHA-384, and SHA-512.

HP | Poly requirements for cryptographic ciphers include:

- Greater than or equal to 128-bit keys for symmetric ciphers.
- Greater than or equal to 2048-bit keys for asymmetric ciphers and Diffie-Hellman key exchange algorithms.
- Greater than or equal to 256-bit curves for Elliptic Curve Cryptography (ECC).

All communication with the Poly Lens portal web servers and client browsers is over a standard secure SSL connection that encrypts all requests and responses. This is achieved with an HTTPS connection that uses TLS 1.2 with a 256-bit encryption layer using SSL and certificates. This connection is encrypted and authenticated using AES_128GCM with ECDH as the key exchange mechanism.

Transport Layer Security (TLS) between components of the Poly Lens is TLS 1.2 for connections, and versions prior to TLS 1.1 are disabled. TLS compression and client-initiated renegotiation also are disabled. Where implemented, secure server renegotiation is compliant with RFC 5746.

Cryptographic cipher suites and modules implemented in Poly Lens are open (publicly disclosed) and have been peer reviewed. Cryptographic libraries are current, regularly updated, and leverage the Advanced Encryption Standard.

Services are architected for High Availability (HA). Services are built to be fault tolerant within the Azure and AWS data centers and each component is made up of multiple instances.

Authentication

Administrators can add additional Poly Lens users by inviting them to a tenant via email. User authentication for Poly Lens can be performed in two ways.

The Poly Lens portal authentication service supports single sign-on (SSO) and can be integrated with the customer's Active Directory via OAuth 2, an authentication protocol that allows users to authenticate for Poly Lens using their enterprise credentials without actually sharing their credentials with HP | Poly. Users will use their Office 365 or ADFS credentials to log into the portal.

Alternatively, users can use Google sign-in to manage the OAuth 2 flow and token lifecycle or create local accounts with email addresses.

Poly Lens Tunnel

When HP | Poly endpoints are configured to send data to Poly Lens, each endpoint establishes an IoT connection to Poly Lens. To configure available options for sending data, please see the Privacy Guide and Administrator's Guide for the specific endpoint device.

A Poly Lens agent on the endpoint uses device-specific credentials to transmit data to Poly Lens using specific ports. All credentials are encrypted via HTTPS tunnel using TLS 1.2. Data is transported and deposited in the Azure data store, located in an SSAE 16 Type II certified Microsoft data center in the United States. All communication between the endpoint and data store is via the encrypted web socket. Any attempt to monitor the link between the agent and data center servers will only show encrypted data packets instead of cleartext information.

Poly Lens Portal

The Poly Lens web portal processes information that the devices have reported to Poly Lens and then presents it to the user.

The following list describes the secure deployment configuration:

- Secure Device IoT connection
- All packets are encrypted
- The socket connection is encrypted

API

You may choose to export data from Lens using an API. When APIs are used, there are two mechanisms for authorizing the API:

- User credentials
- A ClientID & secret for automated actors (machine-to-machine)

The API implements authorization for data access/visibility so you can only see data in your tenant based on your role. This is the exact same API that Lens cloud uses for all data access.

All APIs are encrypted over TLS.

Server Access and Data Security

All customer data sent to Poly Lens cloud service is encrypted both at rest and in transit using strong cryptography including AES-256 and TLS 1.2.

All customer data sent to HP | Poly is backed up daily in digital form using the Azure data factory. Normal access controls of authorized users and data security policies are followed for all backup data. No physical transport of backup media occurs. The backup data during rest and while in transit is encrypted using AES 256. Daily backup snapshots are automated, encrypted, and securely stored.

Servers are in secure data centers, with only authorized staff members having access. The servers are not directly accessible from outside the data centers.

Disaster Recovery and Business Continuity

The Poly Lens cloud service is architected to provide high reliability, resiliency, and security. The service is hosted in multiple Microsoft Azure and Amazon AWS data centers in the United States. Normal low impact outage due to loss of power or connectivity is already handled by the cloud hosting providers — Microsoft Azure and Amazon AWS.

During a major crisis or disaster, service will be moved to a different region until the affected region is restored.

HP | Poly has a Business Continuity and Disaster Recovery Plan reviewed and approved by management to ensure that we are appropriately prepared to respond to an unexpected disaster event. HP | Poly tests disaster recovery processes and procedures on an annual basis but are sometimes conducted more frequently when there are changes to our infrastructure that warrant new tests. We use the results of this testing process to evaluate our preparedness for disasters, and to validate the completeness and accuracy of our policies and procedures.

Security Incident Response

The HP Cybersecurity team promptly investigates reported anomalies and suspected security breaches on an enterprise-wide level. You may contact them directly at informationsecurity@hp.com

The HP Cybersecurity team works proactively with customers, independent security researchers, consultants, industry organizations, and other suppliers to identify possible security issues with Poly products and networks. HP | Poly security advisories and bulletins can be found on the HP Customer Support website.

Subprocessors

HP | Poly uses certain subprocessors to assist in providing our products and services. A subprocessor is a third-party data processor who, on behalf of HP | Poly, processes customer data. Prior to engaging a subprocessor, HP | Poly executes an agreement with the subprocessor that is in accordance with applicable data protection laws.

The subprocessor list here identifies HP | Poly's authorized subprocessors and includes their name, purpose, location, and website. For questions, please contact HP's Chief Privacy and Data Protection Officer form.

Prior to engagement, suppliers that may process data on behalf of HP | Poly must undergo a privacy and security assessment. The assessment process is designed to identify deficiencies in privacy practices or security gaps and make recommendations for reduction of risk. Suppliers that cannot meet the security requirements are disqualified.

Additional Resources

To learn more about Poly Lens, visit our product website.

Disclaimer

This white paper is provided for informational purposes only and does not convey any legal rights to any intellectual property in any HP | Poly product. You may copy and use this paper for your internal reference purposes only. HP | POLY MAKES NO WARRANTIES, EXPRESS OR IMPLIED OR STATUTORY AS TO THE INFORMATION IN THIS WHITE PAPER. THIS WHITE PAPER IS PROVIDED “AS IS” AND MAY BE UPDATED BY HP | POLY FROM TIME TO TIME. To review the most current version of this white paper, please visit our website.

© 2024 HP, Inc. All rights reserved. Poly and the propeller design are trademarks of HP, Inc. The Bluetooth trademark is owned by Bluetooth SIG, Inc., and any use of the mark by HP, Inc. is under license. All other trademarks are the property of their respective owners.